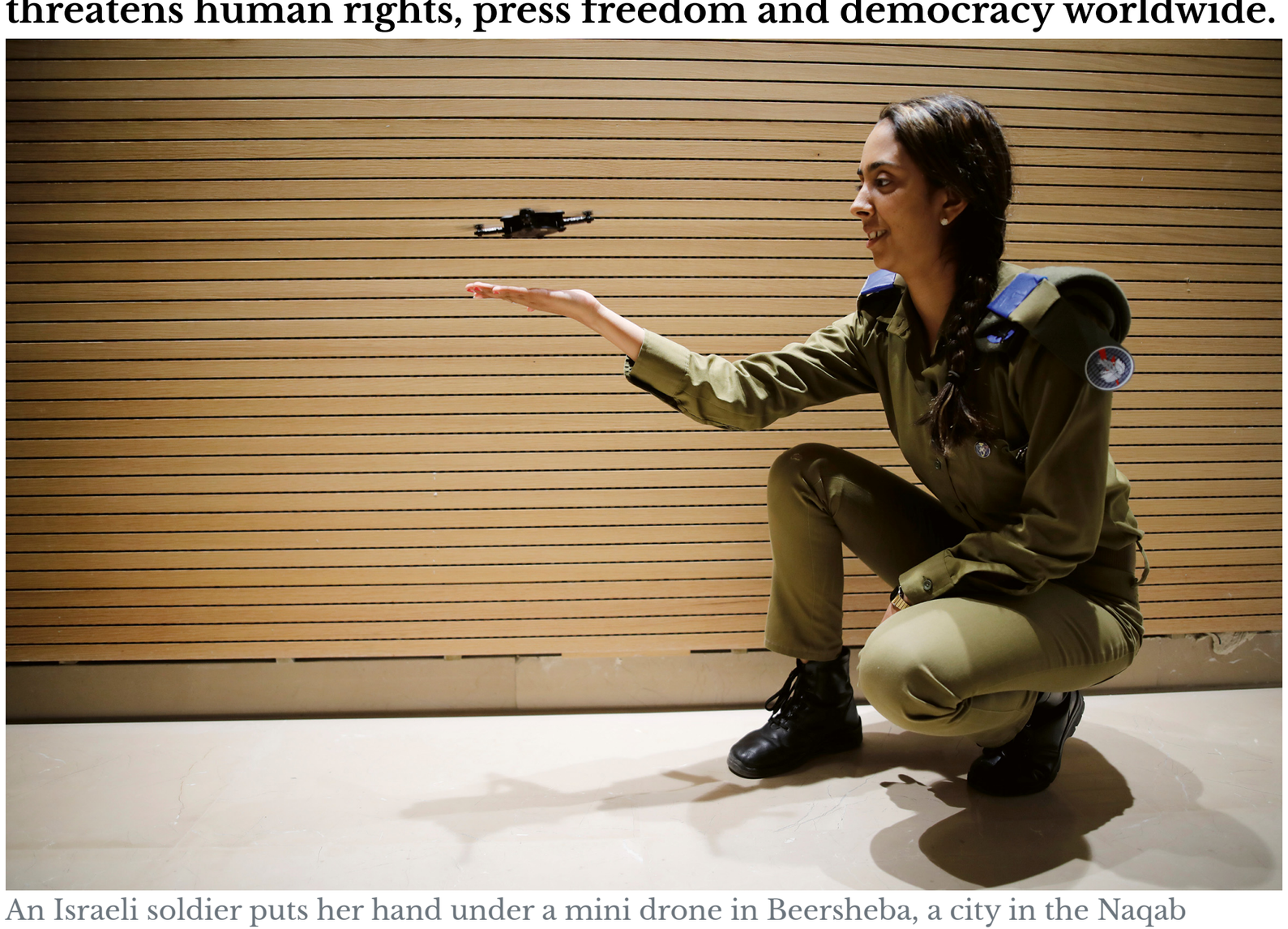
HOW PALESTINE BECAME ISRAEL'S SPYWARE TEST-BED

19 October 2023

Antony Loewenstein

Israel is at the forefront of the booming spyware industry that threatens human rights, press freedom and democracy worldwide.



An Israeli soldier puts her hand under a mini drone in Beersheba, a city in the Naqab desert. In 2022, drones made up 25% of Israel's total weapons exports. AMIR COHEN/REUTERS

Investigative journalist Javier Valdez Cárdenas was gunned down on the streets of Culiacán, northwest Mexico, in May 2017. It was in broad daylight. Just moments beforehand, the reporter had stepped out of the newsroom of *Riodoce*, the Mexican weekly he co-founded to investigate drug cartels. It would be another four years until one of his killers, Juan Francisco Picos Barrueta, was sentenced to 32 years in prison for the crime.

Violence against journalists is all too common in Mexico. But this wasn't a straightforward, brazen execution of a reporter who had dedicated his life to exposing organized crime and corruption. Two years after his death, his widow Griselda Triana, also a journalist, was informed by the Canadian digital watchdog group Citizen Lab that her mobile phone had been infected with a powerful spyware tool called Pegasus. The infection took place 10 days after her husband's killing. Before then Triana had been completely in the dark about any state actors targeting her and Javier. 'Although we had always heard that people could be monitored through cell phones, we did not imagine that this could happen to us,' she said. 'Javier tried to ensure that his conversations on his cell phone were secure.'

I asked Triana why she thought their phones had been infected. 'So [the authorities] could obtain data from sources of information or listen to calls related to his murder,' she replied. It is still not known exactly who was spying on the couple nor why they were targeted, however fingers have been pointed at the Mexican government. It's common for corrupt government officials and drug cartels to work together to eliminate perceived enemies.

The Israeli company behind Pegasus, NSO Group, first displayed its new tool to Mexican authorities in 2011 at a time of heightened drug war violence. While the spyware has been used to fight crime (Pegasus was credited with having secured the 2019 arrest and downfall of the notorious drug cartel chief El Chapo), dozens of journalists, dissidents, political enemies of successive governments and human rights activists have also been targeted, making the Central American country the world's most prolific user of Israeli-made spyware.

GROWING THREAT

A similar story is playing out worldwide. At least 75 states have bought commercial spyware in the last decade. These new surveillance technologies, developed largely by unregulated and opaque private companies, allow the hacker to remotely infiltrate smartphones without the individual's knowledge. Once inside a phone, Pegasus can activate the camera and microphone, as well as steal data, including communications, images and videos. These weapons give governments powers to carry out targeted, invasive surveillance on a scale unimaginable before the advent of such tools. This power has led to horrific abuses. Among the most egregious cases is the Saudi killing in 2018 of *Washington Post* columnist Jamal Khashoggi, who was targeted along with his wife, by Pegasus in the months leading up to his death.

During the research of my new book, *The Palestine Laboratory*, I spoke to Pegasus victims from Togo, Saudi Arabia, Mexico and India. All expressed fears of being watched and the threat of police, gang or military violence. Hacking a phone can uncover every intimate piece of information stored on a device; a victim never feels completely secure again.

'There was panic when Togo activists discovered WhatsApp was breached by Pegasus,' Togolese activist Farida Nabourema told me. 'We thought that the government wasn't that astute, but the dictatorship hires people who are'. The availability of off-the-shelf hacking tools gives states with few resources, such as Togo, the opportunity to pursue high-tech operations – a terrifying prospect for political activists like Farida.

But it's not just dictatorships which are utilizing spyware to target perceived adversaries. In Greece, invasive cyber surveillance tools have been used to snoop on opposition politicians and investigative journalists, triggering a political crisis in the country. As the Cárdenas case in Mexico shows, this new form of electronic surveillance also threatens press freedoms, putting sources at risk, exposing journalists to blackmail and discouraging them from investigative reporting.

So what action has been taken to reign in the insidious spread of the commercial spyware industry? The answer is very little. Despite public outcry sparked by the Pegasus Project revelations – an international investigation into NSO Group which uncovered the scale of spyware abuse in 2021 – there are still no global regulations to control the intrusion industry. In fact, more countries are using commercial spyware today than ever before.

INACTION AND LOOPHOLES

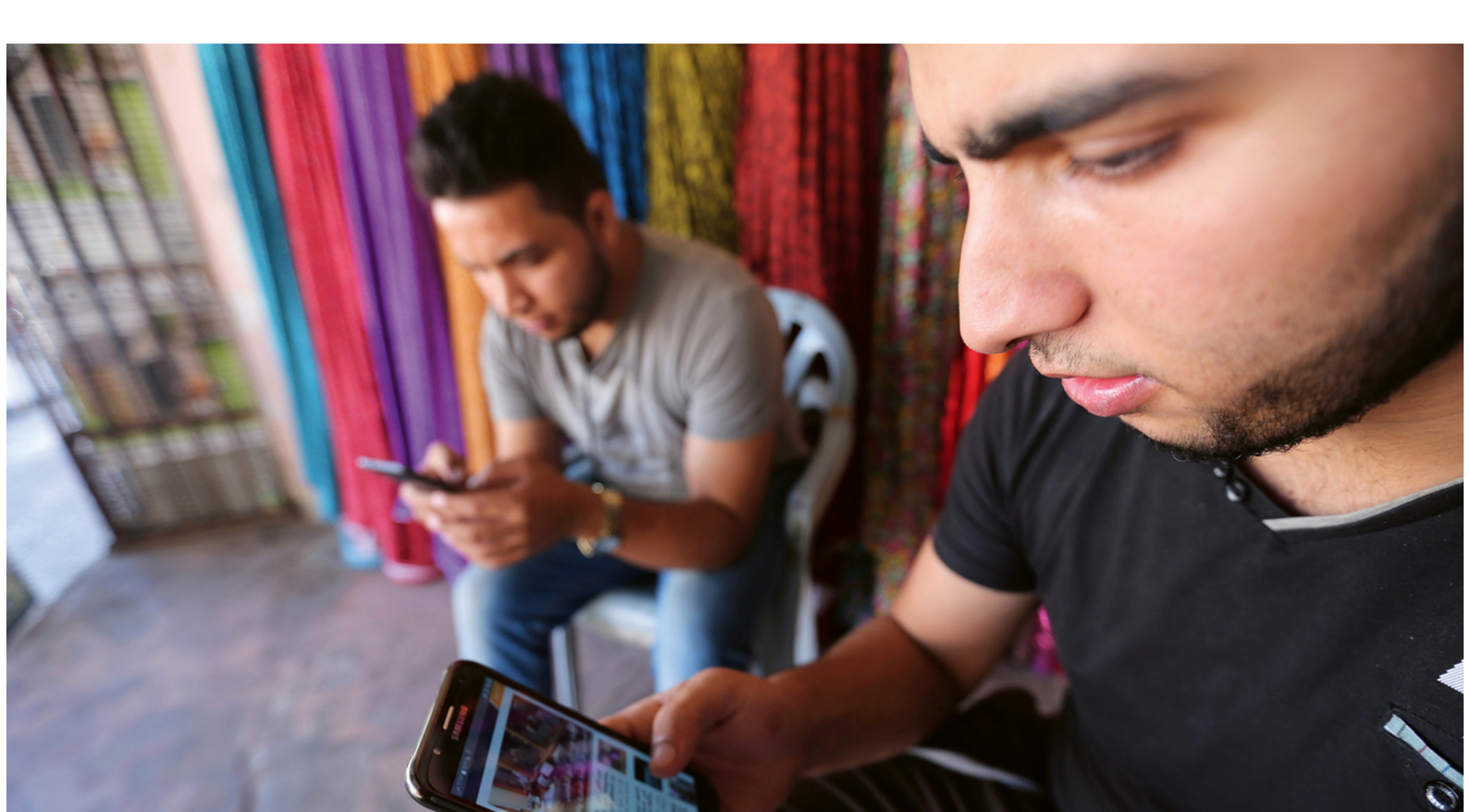
A lack of political will is one of the major drivers fuelling the expansion of the industry. Regulation is sadly not in the interests of governments that wish to obtain and use the intrusive technology for themselves.

> 'When people ask us for something, we cannot afford to ask questions about ideology. The only type of regime that Israel would not aid would be one that is anti-American'

This can be seen within the European Union. While Brussels is flirting with banning the worst spyware companies, so far it's little more than talk. More concrete action has been taken in the US, where President Joe Biden signed an executive order in March restricting the government's ability to use commercial spyware. When announcing the order, the White House noted that the tools had been abused not only by authoritarian regimes but by democracies 'to target their citizens without proper legal authorization, safeguards and oversight'. That followed the decision to sanction NSO Group and another major Israeli spyware firm Candiru in November 2021. Since then, two more European-based hacking companies – Intellexa and Cytrox – have been added to the blacklist. Both firms are run by a former Israeli general, Tal Dilian.

While the ban list has been welcomed by some rights groups, closer inspection of the US's apparent crusade against spyware reveals a different story. Although Pegasus is now officially off the table, other phone hacking tools with similar capabilities are still in use across the country today. According to an analysis by US outlet The Intercept in 2022, all but one of the 15 departments represented in the US cabinet have bought products made by Israeli company Cellebrite in recent years. Meanwhile the US government continued to use the NSO Group product Landmark – a geolocation tool that can secretly track mobile phones around the world – after the 'ban' on the hacking firm was put in place, calling into question the effectiveness and seriousness of the Biden administration's censure.

The executive order also has some major loopholes. For one, it does not cover the use of US intelligence agency-made spyware. In this way, could the blacklist all just be spin to protect Washington's architecture of global spying while neutering a global rival in the hacking game? The US worries that it's losing market share to Israel's booming defence sector, especially since Russia's invasion of Ukraine in early 2022, with many European states lining up to buy missile defence shields, ground-based artillery and rockets. Blacklisting Israeli spyware firms helps puts the US ahead in the hidden battle for cyber weapon dominance between the two powerful nations.



Palestinian men scroll on their smartphones outside a store in Gaza City. The captive population is a 'testing ground' for Israel to develop spyware and surveillance tools it then exports to repressive regimes around the world. IBRAHEEM ABU MUSTAFA/REUTERS

ISRAEL'S INSURANCE POLICY

The lack of serious oversight benefits one actor in particular – Israel. As the lead exporter of these tools, the state is at the forefront of the intrusion technology industry. Founded in 2010, NSO Group Technologies Ltd is just one firm among a wider ecosystem of Israeli cyber-weapons companies. Of the 75 governments that have procured spyware and digital forensic technologies worldwide, 56 bought them from firms that are either based in or connected to Israel, such as NSO Group, Cellebrite, Cytrox and Candiru. These deals are all monitored and approved by the Israeli Ministry of Defence.

For Israel, spyware is not just a highly lucrative industry, but a strategic weapon to curry diplomatic favour. Aside from revolutionizing the world of espionage, the huge demand for these tools is reshaping geopolitics, with Palestinian lives at the sharp end of the sinister global spyware games. According to a *New York Times* investigation, NSO deals have played a central role in securing support from Arab countries, including in the negotiations of the Abraham Accords, the 2020 diplomatic agreements that normalized ties between Israel and Arab states such as Bahrain and the United Arab Emirates. As a result, companies like NSO Group can be viewed as unofficial arms of the Israeli state, furthering the country's military and diplomatic ties.

> 'Without serious global oversight, it's inevitable that the industry will continue to proliferate'

The state's spyware industry has benefited from a revolving door of intelligence officers, in particular Unit 8200, the Israeli army's version of the US National Security Agency (NSA). Having spent their days monitoring every aspect of Palestinian life, that experience has been taken into the private sector where the most sophisticated tools of surveillance are conceived, designed and exported around the world to democracies and dictatorships alike. Occupied Palestinians are the guinea pigs when Israeli weapons of occupation are developed and tested. Spyware is a key part of this picture. Once deployed and 'proven' in the field, Israeli companies promote them as 'battle-tested' in occupied Palestine.

Exporting the tools of the occupation is nothing new. Israel has sold an array of facial recognition tools, 'smart' walls, drones, camera hacking, biometric products and spyware to over 130 nations including Bangladesh, Myanmar, UAE, Saudi Arabia and the Philippines. There are very few nations in the Global South that haven't bought Israeli arms or received Israeli 'counter-insurgency' training.

The most repressive regimes in the last half century have often covertly worked with Israel, from Liberia under dictator William Tubman until his death in 1971, to Guatemala in the 1980s while it was committing genocide against its Indigenous population. The logic behind these relationships was articulated by the former Israeli politician Yohanah Ramati during a speech at Florida International University in March 1985: 'Israel is a pariah state. When people ask us for something, we cannot afford to ask questions about ideology. The only type of regime that Israel would not aid would be one that is anti-American. Also, if we can aid a country that it may be inconvenient for the US to help, we would be cutting off our nose to spite our face not to.' There's rarely been a more honest appraisal of Israel's entire weapons industry.

Although barely discussed in the Western media, Israel's collaboration with dictatorships has been happening since the country came into existence in 1948. One of the main reasons for doing so has been to compliment the American footprint in these regions and serve Washington's interests. Israel wants to exercise leverage over US policy making and remain 'relevant' to its leading benefactor.

Similarly, spyware exports have become an important element of Israel's efforts to protect itself from any official pushback for maintaining, in Palestine, the longest occupation of modern times: 56 years and counting in the West Bank, Gaza, East Jerusalem and the Golan Heights. Israel's arms sector, and its spyware industry in particular, is an insurance policy against political headwinds that may develop against the occupation. Few nations are likely to seriously oppose the brutal oppression of the Palestinian people if they're relying on Israeli weapons. After all, why bite the hand that arms you?

PANDORA'S BOX

While US sanctions have curtailed the power of NSO Group and Candiru, a plethora of other Israeli companies have emerged to fill their place. Without serious global oversight, it's inevitable that the industry will continue to proliferate. Defence Prime is one of the more prominent, founded by Israeli expats living in the US, offering huge amounts of money for the best Israeli hackers. Nonetheless, the allure of NSO Group remains. A range of companies have expressed keen interest in purchasing the corporation. Beyond the brand recognition, demand for spyware is soaring, so whether it's Pegasus or a rival doesn't matter to the activist being targeted.

Enforceable regulation is one solution to the spiralling spyware problem but progress has been slow. An outright ban is a better outcome but there's little political appetite for it. Few, if any, states will accept the possibility of not using powerful cyber-weapons against real or perceived enemies. In 2021, UN human rights experts called for a global moratorium on the sale and transfer of surveillance tools until solid regulation is put in place.

Which country will step up and act responsibly?